REMARKS

I. Status of the Claims

Presently amended claims 6 and 7, and new claims 8 –19 are the only claims pending in this application. Claims 1- 5 are canceled.

II. Substance of the Interview

All items of prior art that the April 20, 2004 Office Action relied upon in rejecting the claims of the present application were discussed. Applicant and Applicant's undersigned counsel submitted that none of the cited items of prior art discloses, teaches or suggests broadcasting a random number sequence, receiving the random number sequence at communication stations, and generating encryption and decryption keys at the communication stations by filling reservoirs at the communication stations with bits sampled, at non-public times, from the received random number sequence. Agreement was reached that upon Applicant amending the claims to more clearly recite the encryption and decryption key generation being based on filling a reservoir with bits sampled at private sampling times from the random number sequence, that the rejections would be withdrawn and, subject to a new search that the Examiner would conduct, the claims would be allowable.

III. Rejections Based On Prior Art

The Office Action rejects the examined claims 1, 6 and 7 under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 5,003,598 ("Kunstadt") in view of M. Rabin, Department of Mathematics, The Hebrew University of Jerusalem, Jerusalem, Israel, "Transaction Protection by Beacons," Journal of Computer and System Sciences 27, 256-267 (1983) ("Rabin").

The Office Action rejects the examined claims 2-5 under 35 U.S.C. § 103 as being unpatentable over Kunstadt, Rabin and U.S. Patent No. 5,161,244 ("Maurer").

Applicant has canceled claims 1-5, without prejudice or disclaimer, for reasons of form. Applicant respectfully submits, however, that the subject matter of the canceled claims 1-5 is patentable over the cited art of record. The subject matter of canceled claim 1 is patentable because the collected teachings of the cited art lack generation of an encryption key based on sampling bits from a publicly broadcast random number sequence. Applicant's arguments, though, are directed at the amended base claim 6, new base claim 8, and new base claim 18, for purposes of advancing this case. Applicant respectfully submits, for reasons presented below, that the amended base claim 6 and new base claims 9 and 18 are patentable over the aggregate teachings of Kunstadt and Rabin and Maurer.

Amended claim 6 and new base claim 9 recite generation and transmission of a random number sequence having significantly greater than N-bits, providing a private key to encryption station, sampling subsequences or bits from the transmitted random number based on the private key, and filling an encryption reservoir based on the sampled subsequences or bits. Amended claim 6 and new claim further recite generating a new sampling time based, at least in part, on the previously sampled bits, sampling the random number sequence based on the new sampling time, and then further filling the encryption reservoir based on the new sampled subsequences or bits. Amended claim 6 and new claim 9 further recite repeating the generation of a new sampling time, sampling the random number sequence based on the new sampling time, and further filling the encryption reservoir, until the reservoir is greater than a predetermined size, the size being based on the N-bits. The N-bit encryption key is then set or established according to the content of the encryption key reservoir.

As described by Applicant's originally filed specification, the sampling times are known only to the encryption station. Therefore, the encryption reservoir is filled with data for an N-bit encryption key, which was selectively extracted at particular, secret sampling times, from a much longer random number sequence. An unintended listener must store a duration of the random number sequence, covering the entire time span over which the secret sampling could have occurred, in order to have sufficient information to conduct a search for the N-bit encryption key. Applicant's described method contemplates that this would exceed the storage capacity of foreseeable unintended listeners.

Kunstadt, Rabin, and Maurer are silent on sampling random bits from the public broadcast. Kunstadt's security key (see Kunstadt, at column 3 Lines 27-31) is used to set the initial start number of the pseudo-random number generator, not the time at which the bits should be extracted from the public broadcast. Rabin does not specify a secret method or a secret time for extracting bits from the random number broadcast, nor does Maurer.

Kunstadt, Rabin, and Maurer do not teach or suggest anything of, or toward, sampling bits from any transmission, much less sampling from a transmitted random number, at times that are known only to the parties. Kunstadt, Rabin, and Maurer do not teach or suggest anything of, filling a reservoir with N bits sampled from a longer random number sequence, by any method, much less sampling based on a private key. Further, the aggregate disclosures of Kunstadt, Rabin, and Maurer do not teach or suggest anything of, filling a reservoir by sampling bits from a random number sequencer at times based on previously sampled bits.

For each of these reasons standing alone, the amended claim 6 and new claim 9 are patentable over the combined teachings Kunstadt, Rabin or Maurer

Applicant's new claim 18 recites generating a random number sequence greater than N bits, providing a private key to a first communication station, and receiving the random number sequence at the first communication station. New claim 18 further recites then repeatedly filling a first reservoir at said first communication station with selected bits from said received random number sequence. Applicant's new claim 18 further recites that each selection is based on at least one of the private key and a value of previously selected bits, until the first reservoir reaches a predetermined threshold based on N. The aggregate disclosures of Kunstadt, Rabin, and Maurer teach nothing of filling a reservoir with sampled bits from a broadcast random number sequence. Further, Kunstadt, Rabin, and Maurer teach nothing of such a filling based on repeated sampling of the random number sequence, by any sampling method, much less by selecting bits based on any of a private key or the value of previously sampled bits. For each of these reasons standing alone, Applicant's new claim 18 is patentable over the combined teachings Kunstadt, Rabin and Maurer.

The Examiner at paragraph 7 of the Office Action states that "[a]s per claim 2, the limitation of generating a synchronization signal is disclosed by Kunstadt using, for example, WWV." Applicant responds that Kunstadt uses the WWV as a source of the reference signal indicating when the pseudo-random number generator must be re-set. The WWV is a possible input to the Kunstadt system, similar to a music or talk radio station. In Applicant's description, and the claims reciting the synchronization signal, the synchronization signal is used as a basis, together with the private key, to set the time for sampling blocks of data from the transmitted random number. This helps insure that both the encrypting and decrypting parties will select the same strings of random bits from a very high bandwidth broadcast. The function, operation, and purpose of Kunstadt's synchronization signal have nothing to do with any sampling time.

The Office Action states at paragraph 11 that "Kunstadt uses keying material extracted an publicly [sic] broadcasted unrelated signal." Applicant respectfully responds that Kunstadt does not extract keying material from the public broadcast. The keying material is generated by a pseudo-random number generator. This generator is cited in the "Other Publications section" and Column 3 Lines 11-15.

The Office Action also states at paragraph 11 that "Kunstadt also discloses a synchronizing means. The extracted feature from the unrelated signal is then used to generate a private key which would indicate the interval." Applicant respectfully responds that Kunstadt is silent on the generation of a private key to indicate an interval. Kunstadt's reference signal is used to re-set a pseudo-random number generator. The output of this generator is used as the keying material. Kunstadt does not extract any material from the public broadcast other than the noted timing reference signal used for the purposes of synchronizing the pseudo-random number generators at the sending and receiving stations.

IV. Conclusion

Applicant respectfully submits, for the reasons presented above, that all pending claims of the present application stand in condition for allowance.

The Examiner is respectfully requested to contact the undersigned, at the telephone number below, if any further action or changes are deemed necessary to expedite this case.

Respectfully submitted,

By ____________ Date: 10/5/2004

Laurence E. Stein,
Reg. No. 35,371
PATTON BOGGS LLP
2550 M Street, N.W.
Washington, D.C. 20037
202-457-6491 (direct)